BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 34 585 A 1**

(51) Int. Cl.[6]:
G 06 F 12/16
G 06 F 12/14
G 06 F 13/12

(21) Aktenzeichen: 197 34 585.9
(22) Anmeldetag: 9. 8. 97
(43) Offenlegungstag: 11. 2. 99

(71) Anmelder:
Brunsch, Hans, 81739 München, DE; Heilos, Hans Christoph, Shailela Newtown, IE

(74) Vertreter:
Schlimme, W., Dipl.-Ing. Dipl.-Wirtsch.-Ing. Dr.-Ing., Pat.-Anw., 85521 Ottobrunn

(72) Erfinder:
Heilos, Hans Christoph, Cobh Co. Cork, IR; Heilos, Hans Christian, Cobh Co. Cork, IR

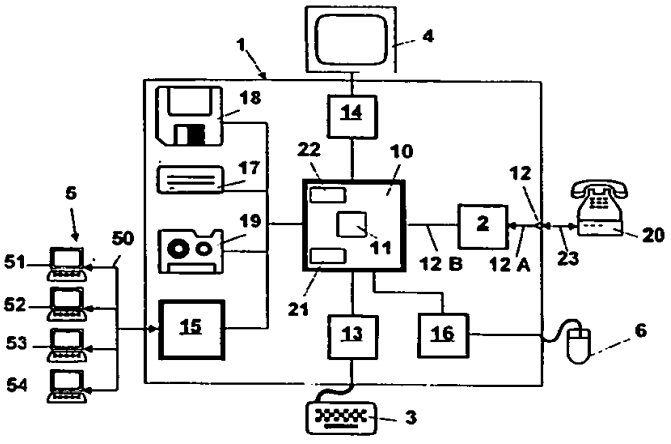
(56) Entgegenhaltungen:
US 55 11 163

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren, Vorrichtung und Softwareprogramm zur Überwachung von Informationsflüssen in Computersystemen

(57) Ein Verfahren zur Überwachung von Informationsflüssen in Computersystemen, wobei Information zwischen zumindest einer ersten Rechnerzentraleinheit und zumindest einer Peripheriegeräteeinheit oder einer weiteren Rechnerzentraleinheit geleitet wird, weist die Schritte auf: Einleiten der Information in in einen Speicher einer Sicherheitsrechnereinrichtung, Bearbeiten der Information in der Sicherheitsrechnereinrichtung nach einer vorgebbaren Bearbeitungsprozedur, Überwachen der durch das Bearbeiten der Information in der Sicherheitsrechnereinrichtung erzeugten Reaktion und Weiterleiten der Information, wenn die erzeugte Reaktion einem vorgegebenen Reaktionsmuster entspricht. Eine Vorrichtung zur Durchführung dieses Verfahrens weist eine Sicherheitsrechnereinrichtung in der Informationsstrecke zwischen der ersten Rechnerzentraleinheit und der Peripheriegeräteeinheit oder weiteren Rechnerzentraleinheit auf, so daß der Fluß der Information durch die Sicherheitsrechnereinrichtung von einem Informationseingang zu einem Informationsausgang erfolgt, wobei die Sicherheitsrechnereinrichtung zumindest einen wiederbeschreibbaren Speicher aufweist, indem zumindest ein Speicherbereich vorgesehen ist, in den eine durch den Informationseingang ankommende Information eingeleitet wird, in dem sie bearbeitet wird und aus dem sie weitergeleitet wird.



DE 197 34 585 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Überwachung von Informationsflüssen in Computersystemen, wobei Information zwischen zumindest einer Rechnerzentraleinheit (CPU) und zumindest einer Peripheriegeräteeinheit oder einer weiteren Rechnerzentraleinheit (CPU) geleitet wird. Weiterhin betrifft die Erfindung eine Vorrichtung zur Überwachung von Informationsflüssen in Computersystemen, wobei Information zwischen zumindest einer ersten Rechnerzentraleinheit (CPU) und zumindest einer Peripheriegeräteeinheit oder einer weiteren Rechnerzentraleinheit (CPU) durch eine Informationsstrecke geleitet wird. Schließlich stellt die Erfindung auch noch ein entsprechendes Softwareprogramm bereit.

Computer und insbesondere Computernetzwerke sind heute verstärkt unerlaubten und erwünschten Angriffen von außen, beispielsweise durch Computerviren oder durch Zugriffsversuche von unautorisierten Personen ausgesetzt, insbesondere wenn die Computer oder die Computernetzwerke mit öffentlichen Netzwerken wie dem Internet verbunden sind. Es ist zwar bekannt, an der Schnittstelle zum öffentlichen Netz eine sogenannte Firewall vorzusehen, die ein Eindringen von unautorisierten Personen, sogenannten Hakkern, in einen Computer oder in ein lokales Computernetzwerk erschweren, doch bieten diese Systeme keinen Schutz gegen Viren und auch nicht gegen das unerlaubte Eindringen von unautorisierten Personen, die Insiderkenntnisse über den Computer oder über das lokale Computernetzwerk und deren Sicherheitsvorkehrungen besitzen.

Gegen Computerviren gibt es zwar Virenschutzprogramme, die ihnen bekannte Viren oder virenähnliche Programmkonstrukte erkennen können, sofern sie den elektronischen Fingerabdruck des entsprechenden Virus "kennen" oder mittels eines Softwarealgorithmus eine ankommende Information auf für Viren typische Programmstrukturen hin untersuchen können. Die Gefahr, daß derartige Virenschutzprogramme versagen, steigt, wenn ein neuer Virus oder eine neue virusähnliche Programmstruktur auftaucht, so daß ein ständiges Aktualisieren der Virenschutzprogramme erforderlich ist, wobei eine Aktualisierung immer nur eine Reaktion auf neue Viren oder Virenarten sein kann.

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren sowie eine Vorrichtung und auch ein Softwareprogramm anzugeben, mittels derer der Schutz von an einem öffentlichen Netz angeschlossenen Computern oder lokalen Computernetzwerken verbessert und damit die Sicherheit erhöht wird.

Der das Verfahren betreffende Teil dieser Aufgabe wird gelöst durch die Verfahrensschritte: Einleiten der Information in einen Speicher einer Sicherheitsrechnereinrichtung, Bearbeiten der Information in der Sicherheitsrechnereinrichtung nach einer vorgebbaren Bearbeitungsprozedur, Überwachen der durch das Bearbeiten der Information in der Sicherheitsrechnereinrichtung erzeugten Reaktion und Weiterleiten der Information, wenn die erzeugte Reaktion einem vorgegebenen Reaktionsmuster entspricht.

Bei diesem erfindungsgemäßen Verfahren wird die ankommende Information zunächst in einem Speicher (z. B. einem Speicherbaustein) abgelegt, der in herkömmlicher Weise über Adressen angesprochen wird. Die Information wird dann mit der vorgebbaren Bearbeitungsprozedur behandelt, das heißt sie wird mit bestimmten Befehlen beaufschlagt und die Reaktion der Information auf diese Befehle, das heißt zum Beispiel ein Zugriff auf eine bestimmte Speicheradresse, wird überwacht und mit einem vorgegebenen Reaktionsmuster verglichen, wodurch festgestellt werden kann, ob diese Reaktion für die untersuchte Information typisch und zulässig ist.

Entspricht die erzeugte Reaktion einem vorgegebenen Reaktionsmuster, so wird die Information aus der Sicherheitsrechnereinrichtung an den Zielrechner oder die Peripheriegeräteeinheit weitergeleitet. Die Information kann beispielsweise eine E-Mail-Nachricht, eine Programmdatei, eine Textdatei, ein Spreadsheet einer Tabellenkalkulation, eine Datenbankdatei oder irgendeine andere Datei sein. Auf diese Weise kann festgestellt werden, ob ein Virus in einer Information einen unerlaubten Speicherzugriff, beispielsweise auf den Boot-Sektor einer Festplatte oder einen unerlaubten Befehl, beispielsweise einen Formatierungsbefehl für eine Festplatte, als Reaktion auf irgendeinen an diese Information gerichteten Befehl, beispielsweise einen Druck- oder Copy-Befehl oder auch nur als Reaktion auf eine Zeit- oder Datumsinformation, ausgibt.

Diese erfindungsgemäße Sicherheitsprozedur kann nicht nur durchgeführt werden, um Zugriffe von außen auf eine Rechnerzentraleinheit zu verhindern, sondern kann ebenfalls benutzt werden, um von einer Rechnerzentraleinheit an eine Peripheriegeräteeinheit oder eine weitere Rechnerzentraleinheit ausgesandte Information zu überprüfen und auf die Zulässigkeit ihres Exports hin zu untersuchen.

Ebenso kann das erfindungsgemäße Verfahren von außen an eine Rechnerzentraleinheit in einer Online-Sitzung gerichtete Befehle prüfen und ihre Weiterleitung an die Rechnerzentraleinheit gegebenenfalls unterbinden, so daß auch unautorisierte Zugriffe von außen nicht mehr möglich sind.

In einer vorteilhaften Ausführungsform wird die Information in einem Sicherheitsspeicherbereich (einem Bereich von Speicheradressen) gespeichert, wenn die erzeugte Reaktion nicht einem vorgegebenen Reaktionsmuster entspricht. Diese auch als "abgelehnte Nachricht" bezeichnete Information wird auf eine sichere Weise derart im Sicherheitsspeicherbereich, vorzugsweise auf einem separaten Speichermedium, abgelegt, daß der Inhalt der Information beispielsweise in einem FTAM-envelope (wie ein Brief in einem Umschlag) nach außen abgeschottet ist. Dabei werden wichtige zu der abgelehnten Nachricht gehörige Informationen mit abgespeichert wie die Reaktion, die zur Bewertung als abzulehnende Nachricht geführt hat, also der "Fehler" der Information, sowie insbesondere bei e-Mail-Nachrichten die Herkunft dieser Nachricht und von wem und zu welchem Zeitpunkt diese Nachricht gesendet worden ist. Vorzugsweise wird somit das gesamte an einer e-Mail-Nachricht hängende Routing-Protokoll mit abgespeichert. Hierdurch können beispielsweise Computerviren isoliert werden und später bei Bedarf analysiert werden, um spezifische Abwehrmaßnahmen gegen einen derartigen Virus entwickeln zu können. Außerdem kann mit dieser Information beispielsweise der Absender einer virusverseuchten Information identifiziert und benachrichtigt oder auf andere Weise verfolgt werden.

Diese erfindungsgemäße Vorrichtung ist unabhängig von dem auf dem Zielrechner laufenden Betriebssystem. Nach außen stellt sich die Sicherheitsrechnereinrichtung als "offenes Rechnersystem" dar und ist für eingehende Informationen und Nachrichten nicht als Sicherheitsrechnereinrichtung erkennbar.

Vorteilhafterweise wird eine Alarmmeldung ausgegeben, wenn die erzeugte Reaktion nicht einem vorgegebenen Reaktionsmuster entspricht. Diese Alarmmeldung kann beispielsweise den Systemadministrator in einem Netzwerk über einen erfolgten Virenangriffsversuch oder den Versuch eines Eindringens in einen Computer oder in ein lokales Netzwerk informieren, so daß der Systemadministrator umgehend zusätzliche Sicherheitsmaßnahmen einleiten kann.

In einer vorteilhaften Weiterbildung werden der für die

Information und deren Bearbeitung reservierte Arbeitsspeicherbereich der Sicherheitsrechnereinrichtung, der für das BIOS der Sicherheitsrechnereinrichtung reservierte Arbeitsspeicherbereich und der für das Betriebssystem der Sicherheitsrechnereinrichtung reservierte Arbeitsspeicherbereich zumindest einmal physikalisch gelöscht und das BIOS und das Betriebssystem der Sicherheitsrechnereinrichtung werden erneut in den Arbeitsspeicher geladen, bevor eine neue Information in die Sicherheitsrechnereinrichtung eingeleitet wird.

Alternativ dazu können die vorgenannten Schritte auch durchgeführt werden, nachdem eine Information in der Sicherheitsrechnereinrichtung entsprechend den eingangs genannten Verfahrensschritten abgearbeitet worden ist. Durch diese alternativen zusätzlichen Verfahrensschritte wird gewährleistet, daß Viren, die sich möglicherweise in einen Arbeitsspeicherbereich der Sicherheitsrechnereinrichtung eingeschlichen haben, mit Sicherheit aus dem Arbeitsspeicherbereich gelöscht werden, bevor eine neue Information geladen und nach dem erfindungsgemäßen Verfahren bearbeitet wird.

Das BIOS und das Betriebssystem der Sicherheitsrechnereinrichtung sind vorzugsweise in einem nicht löschbaren und nicht überschreibbaren Speicherbaustein (z. B. einem EPROM) dauerhaft gespeichert und werden hieraus immer "frisch" in den Arbeitsspeicherbereich geladen.

Vorteilhaft ist auch, wenn die Bearbeitungsprozedur eine für die jeweilige Art der Information typische, vorgegebene Behandlungsroutine aufweist. Auf diese Weise können beispielsweise individuelle Behandlungsroutinen für die Behandlung von Textdateien, Programmdateien, Spreadsheets, Datenbanktabellen oder andere Dateien Anwendung finden.

Weiter vorteilhaft ist es, wenn die Bearbeitungsprozedur einen oder mehrere Befehle einmal oder mehrmals ausführt, die an sich geeignet sind, Virenprogramme oder andere, in der zu behandelnden Information versteckte und somit nicht erkennbare unautorisierte Programme oder Programmroutinen zu aktivieren. Hierdurch wird gewährleistet, daß beispielsweise Viren, die sich erst nach einer gewissen Zeitspanne oder nach einer mehrmaligen Anzahl von Kopierbefehlen oder anderen Befehlen aktivieren, zuverlässig entdeckt werden.

Werden im Schritt des Überwachens der durch das Bearbeiten der Information in der Sicherheitsrechnereinrichtung erzeugten Reaktion Zugriffe auf vorgegebene Adressbereiche im Arbeitsspeicher und/oder in Cachespeichern detektiert und auf ihre Zulässigkeit hin ausgewertet, so können gezielt Virenangriffe oder beabsichtigtes Entwenden von gespeicherten Daten erkannt und unterbunden werden. Die vorgegebenen Adressbereiche können beispielsweise BIOS-Speicherbereiche, Betriebssystem-Speicherbereiche, Netzwerkspeicherbereiche, Grafikkartenspeicherbereiche, Speicherbereiche für Festplatten oder andere Datenträgerlaufwerke sowie sonstige nicht freigegebene Arbeitsspeicherbereiche sein.

Eine andere bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens kennzeichnet sich dadurch, daß die Schritte des Bearbeitens und des Überwachens für bestimmte vorgebbare Information umgangen werden und die Information direkt an einen definierten zulässigen Adressbereich im Arbeitsspeicher und/oder in Cachespeichern weitergeleitet wird und daß die verbleibenden Adressbereiche des Arbeitsspeichers und/oder von Cachespeichern derart überwacht werden, daß die Information den zulässigen Adressbereich nicht verlassen kann. Der Vorteil dieser Weiterbildung des erfindungsgemäßen Verfahrens liegt darin, daß bestimmte autorisierte Zugriffe schnell erfolgen können, da sich nicht die Sicherheits-Bearbeitungsprozedur der vorliegenden Erfindung durchlaufen müssen. So kann beispielsweise der Zugriff auf den Grafikspeicher ungeprüft zugelassen werden, was beispielsweise das sogenannte Surfen in öffentlichen Netzen wie dem Internet ohne zeitliche Verzögerung gestattet und wobei die erfindungsgemäße Sicherheits-Bearbeitungsprozedur erst dann einschreitet, wenn Zugriffe auf andere Adressbereiche erfolgen.

Der die Vorrichtung zur Überwachung gemäß einem erfindungsgemäßen Verfahren betreffend Teil wird dadurch gelöst, daß eine Sicherheitsrechnereinrichtung in der Informationsstrecke zwischen der ersten Rechnerzentraleinheit und der Peripheriegeräteeinheit oder der weiteren Rechnerzentraleinheit vorgesehen ist, so daß der Fluß der Information durch die Sicherheitsrechnereinrichtung von einem Informationseingang zu einem Informationsausgang erfolgt, und daß die Sicherheitsrechnereinrichtung zumindest einen wiederbeschreibbaren Speicher aufweist, wobei ein Speicherbereich vorgesehen ist, in den eine durch den Informationseingang ankommende Information eingeleitet wird, in dem sie bearbeitet wird und aus dem sie weitergeleitet wird.

Diese erfindungsgemäße Vorrichtung ermöglicht das Abfangen einer eingehenden Information, sowie deren Bearbeitung in einem unabhängigen und physikalisch von dem Zielrechner, an den die Information gesandt werden soll, getrennten Speicher, wobei dieser Speicher alle Register (Speicheradressen) des Zielrechners aufweist. Diese Speicheradressen in der Sicherheitsrechnereinrichtung entsprechen dabei jenen Adressen, die im Zielrechner vorgesehen sind und dort sowohl zu computerinternen als auch zu externen Geräten gehören können. Die Steuerung der Bearbeitungsprozedur und die Überwachung der dadurch ausgelösten Reaktion wird dabei von der Rechnerzentraleinheit des Zielrechners durchgeführt.

Die erfindungsgemäße Vorrichtung ist unabhängig von dem auf dem Zielrechner laufenden Betriebssystem, da sie ein eigenständiges Betriebssystem verwenden, das mit allen bekannten Betriebssystemen zusammenarbeiten kann. Nach außen stellt sich die Sicherheitsrechnereinrichtung als "offenes Rechnersystem" dar und ist für eingehende Informationen und Nachrichten nicht als Sicherheitsrechnereinrichtung erkennbar. Das gesamte Rechnersystem des Zielrechners wird in der Sicherheitsrechnereinrichtung abgebildet, wobei die Sicherheitsrechnereinrichtung als eine "Black Box" den Zielrechner simuliert.

Vorteilhafterweise ist die Sicherheitsrechnereinrichtung als eigenständig funktionsfähiger Computer mit einer eigenen Rechnerzentraleinheit (CPU) ausgebildet. Bei dieser Ausführungsform kann die Steuerung der Bearbeitungsprozedur, sowie das Überwachen der dadurch ausgelösten Reaktion ebenfalls in der Sicherheitsrechnereinrichtung, also physikalisch getrennt von der Rechnerzentraleinheit des Zielrechners, durchgeführt werden, wodurch die Sicherheit zusätzlich erhöht wird.

Vorteilhafterweise weist die Sicherheitsrechnereinrichtung eigene Arbeitsspeicher und/oder Cachespeicher auf.

In einer besonders bevorzugten Ausführungsform weist die Sicherheitsrechnereinrichtung zumindest einen nicht löschbaren Speicherbaustein zur Aufnahme von zumindest einem Teil des BIOS und/oder des Betriebssystems für die Durchführung des Überwachungsverfahrens auf. Diese Ausgestaltung erhöht weiterhin die Sicherheit des Systems, da die für die Bearbeitung und Überprüfung erforderlichen Programmteile gegen Manipulation von außen geschützt sind.

Ist der Teil der Informationsstrecke, der die Sicherheitsrechnereinrichtung mit der ersten und/oder der weiteren Rechnerzentraleinheit verbindet, zur optischen Entkoppelung von einer elektrooptischen Verbindung gebildet, so

wird die Sicherheit des Systems weiter erhöht, insbesondere wird eine elektrooptische Anbindung des die Überwachung durchführenden Computers oder Computerbereich an den zu überwachenden Computer oder die zu überwachenden Computerbereiche bevorzugt.

Vorzugsweise ist dabei die elektrooptische Verbindung in, als Hybridbausteine ausgebildete Computerbausteine, vorzugsweise in Speicherbausteine, integriert. Hierdurch kann beispielsweise eine Entkoppelung der Überwachungsprozedur von der Bearbeitungsprozedur erfolgen.

In einer besonders einfachen Ausführungsform ist die Sicherheitsrechnereinrichtung virtuell auf der ersten Rechnerzentraleinheit durch ein Softwareprogramm gebildet, das die Rechnerzentraleinheit, sowie deren Arbeitsspeicher und/oder Cachespeicher benutzt.

Die Erfindung betrifft weiterhin ein Softwareprogramm zur Ausführung auf einer Datenverarbeitungsanlage zumindest umfassend ein Betriebssystem, einen Informationsmanagement-Programmteil, der zu einer Rechnerzentraleinheit hin fließende oder von der Rechnerzentraleinheit weg fließende Information abfängt und in einem definierten Zwischenspeicherbereich ablegt, einen Informationsbearbeitungs-Programmteil, der die zwischengespeicherte Information nach einer vorgegebenen Prüfsequenz bearbeitet, wobei die Information mit Programmbefehlen beaufschlagt wird, einen Überwachungs-Programmteil, der Reaktionen der Information auf die Programmbefehle mit vorgegebenen zulässigen Reaktionen vergleicht einen Informationsmanagement-Programmteil, der zu einer Rechnerzentraleinheit hin fließende oder von der Rechnerzentraleinheit weg fließende Information abfängt und der die Information nach einer vorgegebenen Prüfsequenz bearbeitet, wobei die Information mit Programmbefehlen beaufschlagt wird, einen Überwachungs-Programmteil, der Reaktionen der Information auf die Programmbefehle mit vorgegebenen zulässigen Reaktionen vergleicht und der die Information nach Ablauf der Prüfsequenz weiterleitet, wenn während der Prüfsequenz keine unzulässige Reaktion festgestellt worden ist. Dieses Softwareprogramm gestattet die Durchführung des erfindungsgemäßen Verfahrens in einem Computer.

Vorzugsweise ist weiterhin ein Sicherheits-Programmteil vorgesehen, der, falls eine unzulässige Reaktion festgestellt worden ist, die Information sowie Daten über die unzulässige Reaktion sowie vorzugsweise auch Daten über Herkunftseigenschaften der Information sicher in einem Sicherheitsspeicherbereich ablegt. Durch diese Maßnahme wird gewährleistet, daß eine für den Zielrechner möglicherweise gefährliche Information, die beispielsweise einen Virus enthält, isoliert und sicher abgelegt wird.

Weiter vorzugsweise ist ein Alarmierungs-Programmteil vorgesehen, der ein Alarmsignal an eine Anzeigeeinrichtung ausgibt, sobald eine unzulässige Reaktion festgestellt worden ist. Hierdurch kann beispielsweise ein Systemadministrator eines Netzwerks sofort über eine aufgetretene unzulässige Reaktion informiert werden.

Die vorliegende Erfindung betrifft außerdem einen Datenträger mit einem darauf gespeicherten Softwareprogramm gemäß einem der auf ein Softwareprogramm gerichteten Ansprüche der Erfindung.

Einer der wesentlichen Kerngedanken der vorliegenden Erfindung liegt mithin darin, eine an einen Zielrechner oder Zielcomputer gerichtete Information mit einer für die entsprechende Art der Information typischen Bearbeitungsprozedur zu bearbeiten, um dabei festzustellen, ob diese Information nur zulässige Reaktionen wie beispielsweise Zugriffe auf bestimmte Speicheradressen ausführt oder ob unzulässige Reaktionen auftreten, d. h. beispielsweise versucht wird, auf üblicherweise für eine bestimmte Information nicht benutzte Speicheradressen zuzugreifen, wodurch die Information dann als gefährlich eingestuft und nicht an den Zielrechner weitergeleitet wird.

Die Durchführung des erfindungsgemäßen Verfahrens bzw. der Ablauf des erfindungsgemäßen Softwareprogramms kann entweder auf einem eigenständigen als Hardware ausgebildeten Sicherheitsrechner oder aber auch in einem abgegrenzten Speicherbereich des Zielrechners als virtuell ausgebildete Sicherheitsrechnereinrichtung erfolgen. Es sind auch Zwischenstufen möglich, in denen Teile der Sicherheitsrechnereinrichtung als eigenständige Hardware ausgebildet sind, wie beispielsweise die Speicherbausteine, und andere Teile der Sicherheitsrechnereinrichtung virtuell auf dem Zielrechner gebildet sind, so daß Teile des Zielrechners wie dessen Prozessor für die Durchführung des erfindungsgemäßen Verfahrens bzw. für den Ablauf des erfindungsgemäßen Softwareprogramms mitbenutzt werden.

Die Erfindung wird nachfolgend anhand eines Beispiels unter Bezugnahme auf die Zeichnung näher erläutert; in dieser zeigt:

Fig. 1 den schematischen Aufbau eines Local-Area-Network-Servers, mit Anschluß an ein externes Netzwerk;

Fig. 2 den schematischen Aufbau der im Server aus **Fig.** 1 enthaltenen Sicherheitsrechnereinrichtung;

Fig. 3 ein Flußdiagramm eines erfindungsgemäßen Verfahrens, das auf dem Server nach **Fig.** 1 ausgeführt wird.

In **Fig.** 1 ist der schematische Aufbau eines als Netzwerk-Server für ein lokales Netzwerk LAN (Local-Area-Network) dienenden Computers **1** dargestellt.

Der Computer **1** weist eine Hauptplatine (Motherboard) **10** auf, auf der eine Rechnerzentraleinheit (CPU) **11** in bekannter Weise vorgesehen ist. Der Aufbau der Hauptplatine **10** ist nicht Gegenstand dieser Erfindung und entspricht daher dem einem Fachmann geläufigen üblichen Aufbau. An der Hauptplatine ist über eine Tastaturschnittstelle **13** eine externe Tastatur **3** angeschlossen. Die Hauptplatine **10** ist weiterhin über eine Grafikschnittstelle **14** mit einem Bildschirm **4** verbunden. Mit einer Maus **6** steht die Hauptplatine **10** über eine Zeigegerätschnittstelle **16** in Verbindung. Ebenfalls an der Hauptplatine **10** angeschlossen sind als weitere Peripheriegeräte eine Festplatte **17**, ein Diskettenlaufwerk **18** und ein Bandlaufwerk **19**, sowie eine Netzwerkkarte **15**. Auf der Hauptplatine **10** sind zudem ein Arbeitsspeicher **21** und ein Cachespeicher **22** vorgesehen.

Der Computer **1** steht über die Netzwerkkarte **15**, an der Netzwerkverbindungsleitungen **50** angeschlossen sind, in Verbindung mit weiteren Computern **51, 52, 53, 54** eines lokalen Netzwerkes **5**.

Weiterhin weist der Computer **1** einen Anschluß **12** für eine Verbindungsleitung **23** zu einem Modem **20** auf, über welches der Computer **1** mit einem externen Netzwerk, beispielsweise dem Internet, in Verbindung steht. Anstelle eines Modems können an den Eingang **12** auch andere Verbindungsvorrichtungen angeschlossen sein, die eine Verbindung zwischen dem Computer **1** und einem externen Netzwerk herstellen.

Der Eingang **12** ist über eine Verbindungsleitung **12A, 12B** mit der Hauptplatine **10** und damit auch mit der Rechnerzentraleinheit **11** verbunden. In dieser Verbindungsleitung **12A, 12B** ist eine Sicherheitsrechnereinrichtung **2** vorgesehen, so daß der Eingang **12** über eine erste Verbindungsleitung **12A** mit der Sicherheitsrechnereinrichtung **2** verbunden ist und die Sicherheitsrechnereinrichtung **2** über eine zweite Verbindungsleitung **12B** mit der Hauptplatine **10** verbunden ist. Diese zweite Verbindungsleitung **12B** kann von einem optischen Leiter gebildet sein, der über optoelektronische Wandler mit der Sicherheitsrechnereinrichtung **2** und der Hauptplatine **10** verbunden ist.

Signale, die aus einem externen Netzwerk kommen und in den den Zielrechner bildenden Computer **1** eingeleitet werden, müssen somit zunächst die Sicherheitsrechnereinrichtung **2** passieren, bevor sie an die Hauptplatine **10** und damit an die Rechnerzentraleinheit **11** weitergeleitet werden.

In **Fig. 2** ist der Aufbau einer bevorzugten Sicherheitsrechnereinrichtung **2** dargestellt. Die Sicherheitsrechnereinrichtung **2** besitzt eine Hauptplatine **210**, die in ähnlicher Weise aufgebaut ist, wie die Hauptplatine **10** des Computers **1**. Die Hauptplatine **210** der Sicherheitsrechnereinrichtung **2** weist eine Rechnerzentraleinheit (CPU) **211** und einen Cachespeicher **222** auf. Der Cachespeicher **222** kann auch teilweise oder vollständig in die Rechnerzentraleinheit **211** integriert sein.

Weiterhin weist die Sicherheitsrechnereinrichtung **2** Arbeitsspeicher auf, die in **Fig. 2** als quadratische Kästchen symbolisch dargestellt sind, und die vorzugsweise ebenfalls auf der Hauptplatine **210** angeordnet sind. Zur besseren Darstellung sind diese Arbeitsspeicher jedoch in **Fig. 2** separat eingezeichnet. Diese Arbeitsspeicher oder Arbeitsspeicherbereiche sind jeweils einer Komponente des Computers **1** in **Fig. 1** zugeordnet. Der Arbeitsspeicherbereich **212** ist dem Eingang **12** zugeordnet, der Arbeitsspeicherbereich **213** ist der Schnittstelle **13** für die Tastatur **3** zugeordnet, der Arbeitsspeicherbereich **214** ist der Grafikschnittstelle **14** für den Bildschirm **4** zugeordnet, der Arbeitsspeicherbereich **215** ist der Netzwerkkarte **15** zugeordnet, der Arbeitsspeicherbereich **219** ist dem Bandlaufwerk **19** zugeordnet, der Arbeitsspeicherbereich **217** ist der Festplatte zugeordnet, der Arbeitsspeicherbereich **218** ist dem Diskettenlaufwerk **18** zugeordnet und der Arbeitsspeicherbereich **216** ist der Schnittstelle **16** für das Zeigegerät **6** zugeordnet. Diese Zuordnung erfolgt derart, daß die jeweiligen Arbeitsspeicherbereiche **212, 213, 214, 215, 216, 217, 218, 219, 222** jeweils den gleichen Arbeitsspeicher-Adressbereich aufweisen, wie die ihnen jeweils zugeordneten Komponenten **12, 13, 14, 15, 16, 17, 18, 19, 22** des Computers **1**.

Die Sicherheitsrechnereinrichtung **2** weist auch einen nicht löschbaren und nicht überschreibbaren Speicher **220** auf, der beispielsweise von einem EPROM gebildet ist und in dem das BIOS sowie das Betriebssystem für die Sicherheitsrechnereinrichtung **2** gespeichert sind. Vorzugsweise ist im nicht löschbaren und nicht überschreibbaren Speicher **220** auch ein Überwachungsprogramm für die Durchführung der Überwachung von Reaktionen einer in der Sicherheitsrechnereinrichtung **2** bearbeiteten Information abgespeichert. Die Adressbereiche des Arbeitsspeichers, die nicht zu den vorstehend aufgezählten Adressbereichen gehören, sind schematisch als Arbeitsspeicher **221** auf der Hauptplatine **210** dargestellt.

Eine Überwachungseinrichtung **225** ist ebenfalls in der Sicherheitsrechnereinrichtung **2** vorgesehen und ist mit der Hauptplatine **210** und somit mit der Rechnerzentraleinheit **211** verbunden. Die Überwachungseinrichtung **225** steht außerdem mittels in **Fig. 2** gestrichelt gezeichneter Überwachungsleitungen **223, 224** mit den vorgenannten Bereichen **212, 213, 214, 215, 216, 217, 218, 219** sowie **221** des Arbeitsspeichers, sowie mit dem Cachespeicher **222** in Verbindung. Weitere Überwachungsleitungen **226, 227** führen von der Überwachungseinrichtung **225** zum nicht löschbaren und nicht überschreibbaren Speicher **220**, sowie zur Rechnerzentraleinheit **211**.

Die Überwachungsleitungen **223, 224, 226, 227** können als optische oder optoelektronische Verbindungen ausgebildet sein, wobei nicht gezeigte optoelektrische Wandler in den jeweiligen Speicherbereichen auftretende elektrische Signale in optische Impulse umwandeln, die zur Überwachungseinrichtung **225** geleitet und dort ausgewertet werden.

Die in **Fig. 2** gezeigte Sicherheitsrechnereinrichtung **2** kann entweder direkt auf elektrische Weise oder indirekt auf optische oder optisch entkoppelte Weise über die Leitung **12B** mit der Hauptplatine **10** des Computers **1** verbunden sein. Dabei werden lediglich die Informationen über den Eingang einer neuen Information oder Nachricht, über die Tatsache, daß in der Sicherheitsrechnereinrichtung **2** gerade eine Prüfung einer derartigen Information oder Nachricht durchgeführt wird, darüber, daß diese Überprüfung abgeschlossen ist, und über das Ergebnis der Überprüfung über den Rechnerbus an den Zielrechner übertragen. In beiden Fällen wird die sichere Speicherung einer als gefährlich eingestuften Information oder Nachricht, die auch als "abgelehnte Nachricht" bezeichnet wird, in der Sicherheitsrechnereinrichtung **2** durchgeführt, wozu beispielsweise ein gesicherter Bereich des Arbeitsspeichers **221** reserviert sein kann.

Die Steuerung des gesamten Verfahrens, also der Überprüfung einer Information oder Nachricht, also insbesondere das Bearbeiten der Information oder Nachricht und das Überwachen der durch das Bearbeiten erzeugten Reaktion, erfolgt intern in der Sicherheitsrechnereinrichtung **2**. Ebenso erfolgt die Entscheidung, ob die Nachricht an den Zielrechner weitergeleitet oder sicher gespeichert wird, in der Sicherheitsrechnereinrichtung. Die Überwachung des Löschens der Speicher in der Sicherheitsrechnereinrichtung **2** und die Weiterleitung der als positiv beurteilten getesteten Information oder Nachricht erfolgt über auf dem Zielrechner laufende Software.

Die Sicherheitsrechnereinrichtung **2** kann auch außerhalb des Computers **1** vorgesehen sein und als eigenständiger Computer ausgebildet sein, der zwischen dem Eingang **12** des Computers **1** und dem Modem **20** vorgesehen ist und beispielsweise über eine Leitung des lokalen Netzwerkes mit dem Computer **1** verbunden ist. In diesem Fall wird die Weiterleitung einer akzeptierten Nachricht an den Zielrechner, den Computer **1**, über das lokale Netzwerk durchgeführt, während in der in **Fig. 2** dargestellten Ausführungsform die Weiterleitung einer akzeptierten Nachricht über den Rechnerbus erfolgen kann. Auch die sichere Speicherung einer abgelehnten Nachricht kann in diesem Fall über den Rechnerbus durchgeführt werden und im Computer **1** erfolgen.

In einer weiter vereinfachten Ausführungsform sind lediglich die Speicherbereiche **212, 213, 214, 215, 216, 217, 218, 219, 221** und **222** auf einer separaten Platine oder Einschubkarte des Computers **1** vorgesehen, die über das computerinterne BUS-System mit der Hauptplatine **10** des Computers **1** verbunden sind. Weiterhin weist diese Sicherheitsrechnerplatine den nicht löschbaren und nicht überschreibbaren Speicher **220** mit dem darin enthaltenen Überprüfungs-BIOS, dem Bearbeitungs- und Überwachungsprogramm, sowie dem Programm für die Durchführung der Speicherlöschung auf. Die Steuerung des gesamten Prüfungsablaufes in der auf diese Weise vereinfachten Sicherheitsrechnereinrichtung sowie die Entscheidung über die Qualität der eingegangenen Nachricht erfolgen über eine auf dem Computer **1** selbst laufende Software, wobei die entsprechende Hardware des Computers **1** verwendet wird.

In einer noch weiter vereinfachten Ausführungsform der Erfindung wird die Sicherheitsrechnereinrichtung vollständig auf dem Zielrechner, dem Computer **1**, durch entsprechende Software simuliert, ohne das eine zusätzliche Hardware-Sicherheitsrechnereinrichtung **2** vorgesehen ist. Dabei wird somit die Sicherheitsrechnereinrichtung **2** als "virtuelle Maschine" auf dem Computer **1** abgebildet. Zur Sicherstel-

lung eines maximalen Schutzes werden zum Zeitpunkt des Beginns eines erfindungsgemäßen Überwachungsprozesses alle auf dem Computer **1** laufenden anderen Prozesse angehalten, eingefroren und gespeichert, so daß während des Überwachungsprozesses ausschließlich dieses Überwachungsprogramm auf dem Computer **1** abläuft. Erst wenn der Überwachungsprozeß beendet ist und die zu überprüfende Nachricht beurteilt und entsprechend abgespeichert worden ist, werden die angehaltenen Prozesse wieder weitergeführt.

Bei Verwendung dieser reinen Softwarelösung der Erfindung können die Speicher des Computers **1** Signalerzeuger enthalten, die bei Zugriff auf diese Speicher ein Signal generieren, das von der entsprechenden Überwachungsprozedur ausgewertet wird. Diese Speicher mit Signalerzeugern entsprechen im wesentlichen jenen, die auch in der als Hardwarelösung ausgebildeten Sicherheitsrechnereinrichtung **2** vorgesehen sein können.

In **Fig. 3** ist ein Flußdiagramm gezeigt, welches den Ablauf einer Überprüfungsroutine für eine eingehende Nachricht oder Information darstellt. Dieser Ablauf kann sowohl bei einer Hardwarelösung als auch bei einer reinen Softwarelösung als auch bei gemischten Hard- und Softwarelösungen des erfindungsgemäßen Verfahrens bzw. des erfindungsgemäßen Softwareprogramms realisiert sein.

Zunächst wird im Schritt **100** festgestellt, daß eine Nachricht oder Information im Sicherheitsrechner eingegangen ist. Daraufhin wird im Schritt **101** die Sicherheitsrechnereinrichtung gestartet. Danach werden zunächst die Speicher der Sicherheitsrechnereinrichtung gelöscht (Schritt **102**), was vorzugsweise durch Überschreiben aller Speicheradressen mit Nullen erfolgt. Anschließend werden im Schritt **103** das BIOS, das Betriebssystem und das Überwachungsprogramm aus dem nicht löschbaren und nicht überschreibbaren Speicher **220** in den Arbeitsspeicher **221** geladen. In einem nächsten Schritt **104** wird die eingegangene Nachricht oder Information ebenfalls in den Arbeitsspeicher **221** eingelesen. Es erfolgt daraufhin im Schritt **105** die Bearbeitung der eingelesenen Nachricht oder Information, wobei die Nachricht oder Information mit einer Vielzahl von Befehlen nacheinander beaufschlagt wird. Im Schritt **106** wird dann die Reaktion der Nachricht oder Information auf die im Schritt **105** erfolgte Beaufschlagung mit einem Befehl überwacht. Dabei werden in erster Linie die Zugriffe der Nachricht oder Information auf Speicheradressen beobachtet, analysiert und mit zulässigen Reaktionen (das heißt zulässigen Speicherzugriffen) verglichen, woraufhin im Schritt **107** eine Entscheidung darüber erfolgt, ob die jeweilige Reaktion zulässig ist oder nicht. Ist die beobachtete Reaktion unzulässig, wird im Schritt **108** eine Alarmmeldung erzeugt und die Nachricht oder Information wird in einem sicheren Speicherbereich abgelegt (Schritt **109**). Danach werden alle Speicher gelöscht (Schritt **110**) und die Sicherheitsrechnereinrichtung ist bereit, auf den Eingang einer neuen Nachricht oder Information zu warten.

Wurde die beobachtete Reaktion im Schritt **107** als zulässig erkannt, so wird in einem nächsten Schritt **111** ermittelt, ob die Bearbeitungsprozedur bereits beendet ist, das heißt, ob alle Befehle der Bearbeitungsprozedur bereits ausgeführt worden sind. Ist dies nicht der Fall, wird zum Schritt **105** zurückgekehrt. Ist die Bearbeitungsprozedur jedoch beendet, so erfolgt im Schritt **112** die Weiterleitung der eingegangenen Nachricht oder Information an den Zielrechner, den Computer **1**, bzw. eine temporäre Speicherung der eingegangenen Nachricht oder Information, falls die Sicherheitsrechnereinrichtung als reine Softwarelösung virtuell auf dem Zielrechner, dem Computer **1**, ausgebildet ist. Danach erfolgt im Schritt **110** die Löschung der Speicher, und die Sicherheitsrechnereinrichtung geht in einen Wartezustand über, wo sie für die Aufnahme einer nächsten Nachricht oder Information bereit ist.

Patentansprüche

1. Verfahren zur Überwachung von Informationsflüssen in Computersystemen, wobei Information zwischen zumindest einer ersten Rechnerzentraleinheit (CPU) und zumindest einer Peripheriegeräteeinheit oder einer weiteren Rechnerzentraleinheit (CPU) geleitet wird, mit den folgenden Schritten:
   - Einleiten der Information in einen Speicher einer Sicherheitsrechnereinrichtung,
   - Bearbeiten der Information in der Sicherheitsrechnereinrichtung nach einer vorgebbaren Bearbeitungsprozedur,
   - Überwachen der durch das Bearbeiten der Information in der Sicherheitsrechnereinrichtung erzeugten Reaktion und
   - Weiterleiten der Information, wenn die erzeugte Reaktion einem vorgegebenen Reaktionsmuster entspricht.

2. Verfahren nach Anspruch 1 mit dem weiteren Schritt:
   - Speichern der Information in einem sicherheitsspeicherbereich, wenn die erzeugte Reaktion nicht einem vorgegebenen Reaktionsmuster entspricht.

3. Verfahren nach Anspruch 1 oder 2 mit dem weiteren Schritt:
   - Ausgeben einer Alarmmeldung, wenn die erzeugte Reaktion nicht einem vorgegebenen Reaktionsmuster entspricht

4. Verfahren nach Anspruch 1, 2 oder 3 mit den zusätzlichen Schritten:
   - zumindest einmaliges physikalisches Löschen
     - des für die Information und deren Bearbeitung reservierten Arbeitsspeicherbereichs der Sicherheitsrechnereinrichtung,
     - des für das BIOS der Sicherheitsrechnereinrichtung reservierten Arbeitsspeicherbereichs und
     - des für das Betriebssystem der Sicherheitsrechnereinrichtung reservierten Arbeitsspeicherbereichs

   sowie
   - erneutes Laden des BIOS und des Betriebssystem der Sicherheitsrechnereinrichtung in den Arbeitsspeicher,

   bevor eine neue Information in die Sicherheitsrechnereinrichtung eingeleitet wird.

5. Verfahren nach Anspruch 1, 2 oder 3 mit den zusätzlichen Schritten:
   - zumindest einmaliges physikalisches Löschen
     - des für die Information und deren Bearbeitung reservierten Arbeitsspeicherbereichs der Sicherheitsrechnereinrichtung,
     - des für das BIOS der Sicherheitsrechnereinrichtung reservierten Arbeitsspeicherbereichs und
     - des für das Betriebssystem der Sicherheitsrechnereinrichtung reservierten Arbeitsspeicherbereichs

   sowie
   - erneutes Laden des BIOS und des Betriebssystem der Sicherheitsrechnereinrichtung in den Arbeitsspeicher, nachdem eine Information in der Sicherheitsrechnereinrichtung entsprechend den

Schritten gemäß einem der Ansprüche 1 bis 3 abgearbeitet worden ist.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Bearbeitungsprozedur eine für die jeweilige Art der Information typische, vorgegebene Behandlungsroutine aufweist.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Bearbeitungsprozedur einen oder mehrere Befehle einmal oder mehrmals ausführt, die geeignet sind, Virenprogramme oder andere, aufgrund der zu behandelnden Information nicht erkennbare, unautorisierte Programme oder Programmroutinen zu aktivieren.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei im Schritt des Überwachens der durch das Bearbeiten der Information in der Sicherheitsrechnereinrichtung erzeugten Reaktion Zugriffe auf vorgegebene Adressbereiche im Arbeitsspeicher und/oder in Cachespeichern detektiert und auf ihre Zulässigkeit hin ausgewertet werden.

9. Verfahren insbesondere nach einem der vorhergehenden Ansprüche, wobei die Schritte des Bearbeitens und des Überwachens für bestimmte vorgebbare Information umgangen werden und die Information direkt an einen definierten zulässigen Adressbereich im Arbeitsspeicher und/oder in Cachespeichern weitergeleitet wird und wobei die verbleibenden Adressbereiche des Arbeitsspeichers und/oder von Cachespeichern derart überwacht werden, daß die Information den zulässigen Adressbereich nicht verlassen kann.

10. Vorrichtung zur Überwachung von Informationsflüssen in Computersystemen, wobei Information zwischen zumindest einer ersten Rechnerzentraleinheit (CPU) (11) und zumindest einer Peripheriegeräteeinheit (20) oder einer weiteren Rechnerzentraleinheit (CPU) durch eine Informationsstrecke (12A, 12B, 23) geleitet wird, gemäß einem Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet,

daß eine Sicherheitsrechnereinrichtung (2) in der Informationsstrecke (12A, 12B, 23) zwischen der ersten Rechnerzentraleinheit (11) und der Peripheriegeräteeinheit (20) oder der weiteren Rechnerzentraleinheit vorgesehen ist, so daß der Fluß der Information durch die Sicherheitsrechnereinrichtung (2) von einem Informationseingang zu einem Informationsausgang erfolgt, und

daß die Sicherheitsrechnereinrichtung (2) zumindest einen wiederbeschreibbaren Speicher aufweist, wobei ein Speicherbereich (221) vorgesehen ist, in den eine durch den Informationseingang ankommende Information eingeleitet wird, in dem sie bearbeitet wird und aus dem sie weitergeleitet wird.

11. Vorrichtung nach Anspruch 10, dadurch gekennzeichnet,

– daß die Sicherheitsrechnereinrichtung (2) als eigenständig funktionsfähiger Computer mit einer eigenen Rechnerzentraleinheit (CPU) (211) ausgebildet ist.

12. Vorrichtung nach Anspruch 10 oder 11, dadurch gekennzeichnet,

– daß die Sicherheitsrechnereinrichtung (2) eigene Arbeitsspeicher (212, 213, 214, 215, 216, 217, 218, 219, 221) und/oder Cachespeicher (222) aufweist.

13. Vorrichtung nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet,

– daß die Sicherheitsrechnereinrichtung (2) zumindest einen nicht löschbaren und nicht überschreibbaren Speicherbaustein (220) zur Aufnahme von zumindest einem Teil des BIOS und/oder des Betriebssystems für die Durchführung des Überwachungsverfahrens aufweist.

14. Vorrichtung nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet,

– daß der Teil (12A) der Informationsstrecke, der die Sicherheitsrechnereinrichtung (2) mit der ersten (11) und/oder der weiteren Rechnerzentraleinheit verbindet, zur optischen Entkoppelung von einer elektrooptischen Verbindung gebildet ist.

15. Vorrichtung nach Anspruch 14, dadurch gekennzeichnet,

– daß die elektrooptische Verbindung in als Hybridbausteine ausgebildete Computerbausteine, vorzugsweise in Speicherbausteine, integriert ist.

16. Vorrichtung nach Anspruch 10, dadurch gekennzeichnet,

– daß die Sicherheitsrechnereinrichtung virtuell auf der ersten Rechnerzentraleinheit (11) durch ein Softwareprogramm gebildet ist, das die Rechnerzentraleinheit (11) sowie deren Arbeitsspeicher (21) und/oder Cachespeicher (22) benutzt.

17. Softwareprogramm zur Ausführung auf einer Datenverarbeitungsanlage zumindest umfassend

– ein Betriebssystem;

– einen Informationsmanagement-Programmteil, der zu einer Rechnerzentraleinheit hinfließende oder von der Rechnerzentraleinheit wegfließende Information abfängt und in einem definierten Zwischenspeicherbereich ablegt;

– einen Informationsbearbeitungs-Programmteil, der die zwischengespeicherte Information nach einer vorgegebenen Prüfsequenz bearbeitet, wobei die Information mit Programmbefehlen beaufschlagt wird;

– einen Überwachungs-Programmteil, der Reaktionen der Information auf die Programmbefehle mit vorgegebenen zulässigen Reaktionen vergleicht und der die Information nach Ablauf der Prüfsequenz weiterleitet, wenn während der Prüfsequenz keine unzulässige Reaktion festgestellt worden ist.

18. Softwareprogramm nach Anspruch 17, dadurch gekennzeichnet,

– daß weiterhin ein Sicherheits-Programmteil vorgesehen ist, der, falls eine unzulässige Reaktion festgestellt worden ist, die Information sowie Daten über die unzulässige Reaktion sowie vorzugsweise auch Daten über Herkunftseigenschaften der Information sicher in einem Sicherheitsspeicherbereich ablegt.

19. Softwareprogramm nach Anspruch 17 oder 18, dadurch gekennzeichnet,

– daß weiterhin ein Alarmierungs-Programmteil vorgesehen ist, der ein Alarmsignal an eine Anzeigeeinrichtung ausgibt, sobald eine unzulässige Reaktion festgestellt worden ist.

20. Datenträger mit einem darauf gespeicherten Softwareprogramm gemäß einem der Ansprüche 17 bis 19.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 197 34 585 A1
Int. Cl.[6]: G 06 F 12/16
Offenlegungstag: 11. Februar 1999

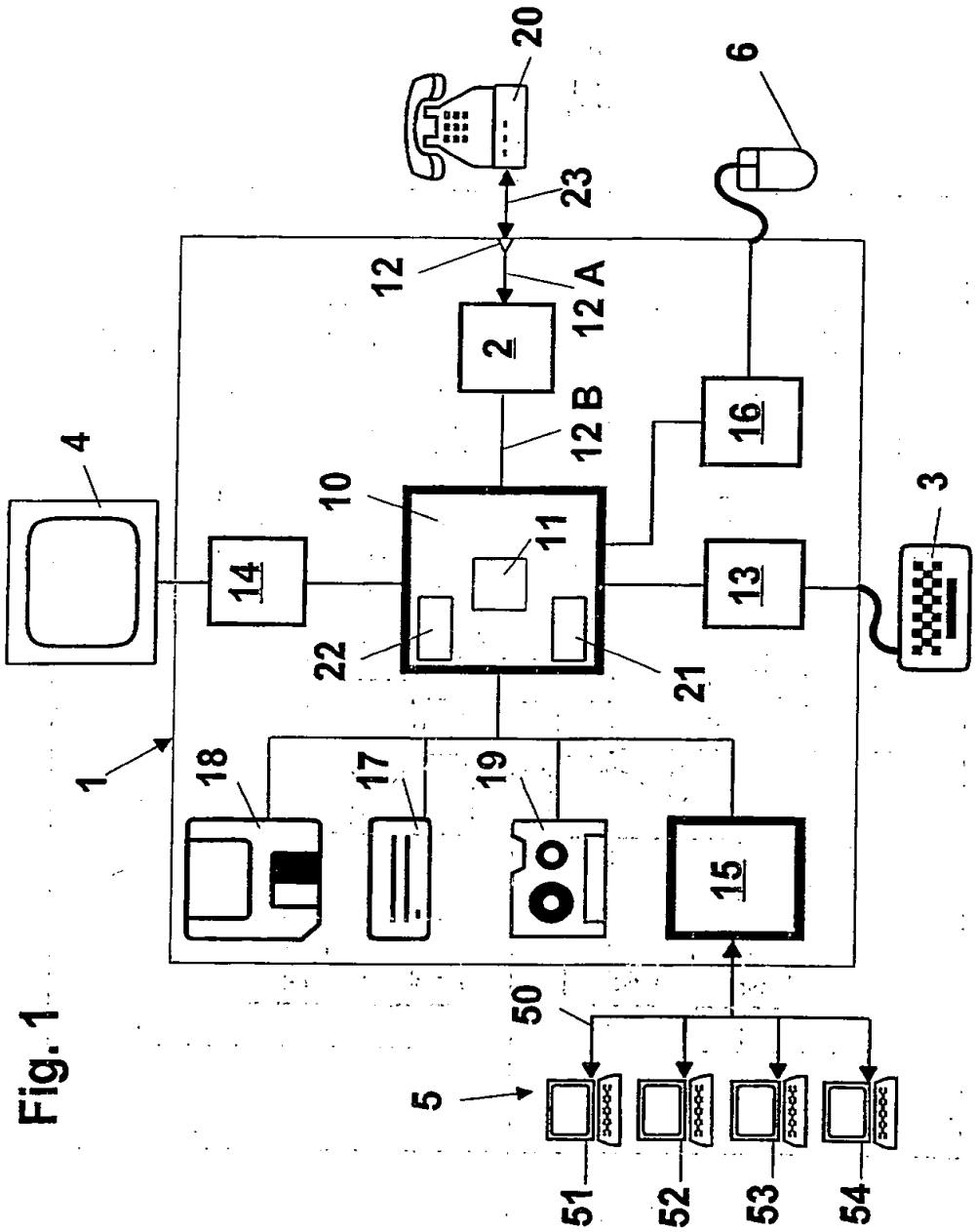


Fig. 1

Nummer: DE 197 34 585 A1
Int. Cl.[6]: G 06 F 12/16
Offenlegungstag: 11. Februar 1999

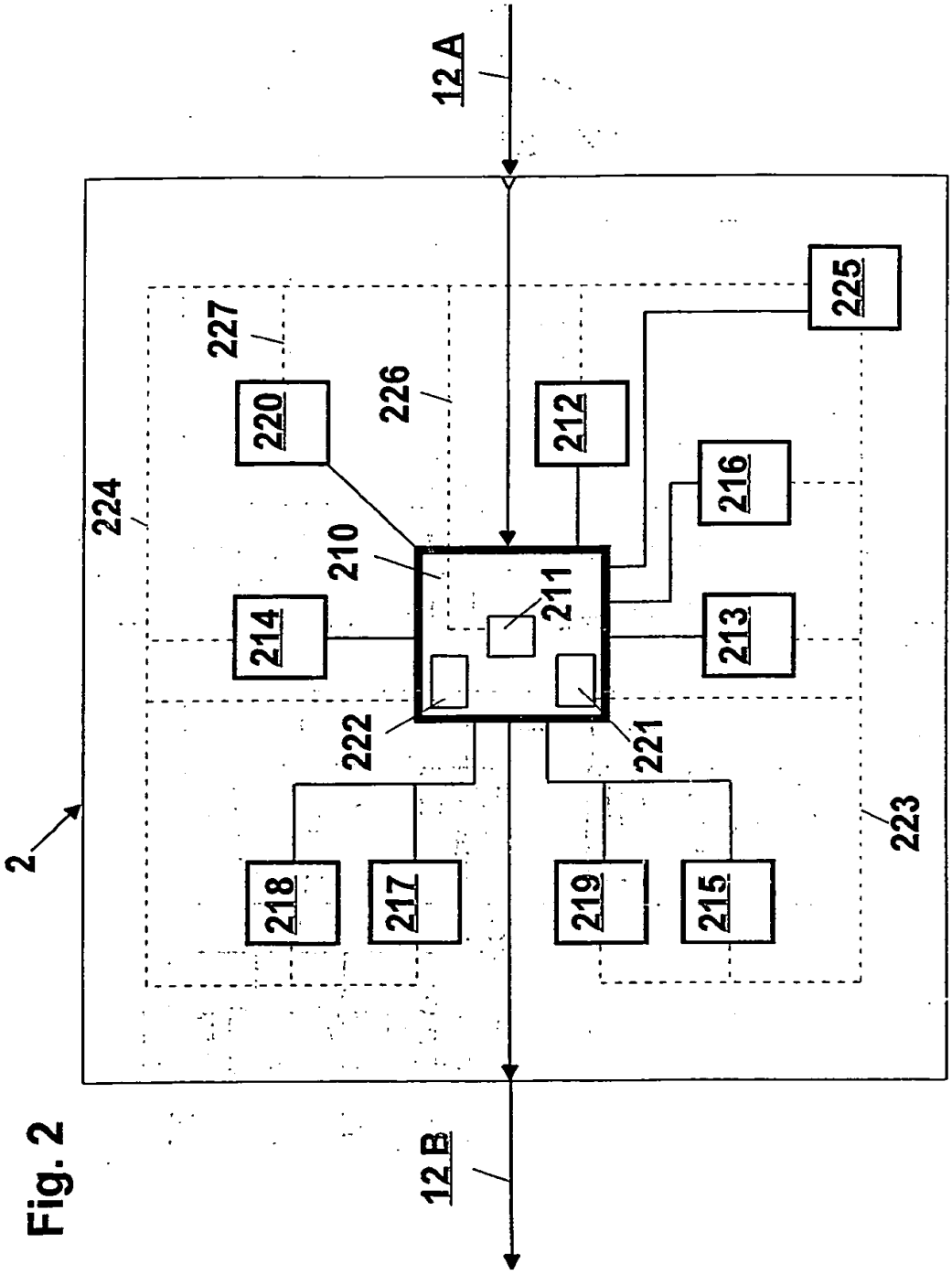


Fig. 2

Nummer: DE 197 34 585 A1
Int. Cl.[6]: G 06 F 12/16
Offenlegungstag: 11. Februar 1999

Fig. 3